Shavlik Protect

Guia de Atualização

shavlik

Copyright

Marcas comerciais

Informações do documento e Histórico de impressão

Número do documento: N/A

Data	Versão	Descrição
Setembro de 2010	NetChk Protect 7.6	Atualizar a marca do produto, adicionar as informações sobre os novos recursos e melhorias do 7.6.
Março de 2011	NetChk Protect 7.8	Adicionar as informações sobre os novos recursos e melhorias do 7.8.
Outubro de 2011	VMware vCenter Protect 8.0	Atualizar a marca do produto, adicionar as informações sobre as tarefas de atualização do 8.0. Remover todas as informações sobre as versões anteriores à 7.5.
Dezembro de 2011	Vmware vCenter Protect 8.0, Documento Rev A	Adicionar o passo explicando como compactar o banco de dados antes de iniciar o processo de atualização.
Setembro de 2012	Vmware vCenter Protect 8.0.1	Atualizar o nome do produto e versão, atualizar abrange os gráficos.
Maio de 2013	Shavlik Protect 9.0	Atualizar os requisitos do sistema. Adicionar as informações sobre os novos recursos e melhorias da v9.0.
Abril de 2014	Shavlik Protect 9.1	Atualizar os requisitos do sistema. Adicionar as informações sobre os novos recursos e melhorias da v9.1.
Setembro de 2015	Shavlik Protect 9.2	Atualizar os requisitos do sistema. Adicionar as informações sobre os novos recursos e melhorias da v9.2.

BEM-VINDO

Finalidade desta Guia

Bem-vindo ao Shavlik Protect 9.2. Este documento descreve como atualizar do Shavlik Protect 9.0 ou do Shavlik Protect 9.1 para o Shavlik Protect 9.2.

Além de descrever o procedimento de atualização, este documento lista uma série de diferenças funcionais sobre as quais você deve estar ciente quando atualizar para o Shavlik Protect 9.2. Este documento também destaca as áreas da interface do usuário que mudaram significativamente.

Novos Requisitos e Pré-requisitos do Sistema

Observe a seguir os novos requisitos e pré-requisitos para o Shavlik Protect 9.2.

- O Windows 2000 não é mais um sistema operacional suportado em máquinas-cliente.
- O Windows 10 (edições Pro ou Enterprise) agora é suportado em máquinas-cliente.

Todos os pré-requisitos de software ausentes serão instalados automaticamente durante o processo de atualização. Consulte a *Guia de Instalação do Shavlik Protect* para a lista completa de requisitos do sistema.

Requisitos da Conta do Usuário para Executar uma Atualização

Para executar uma atualização a sua conta de usuário deve atender aos seguintes requisitos:

- O usuário que executa a atualização do banco de dados deve ser um membro da função db_owner.
- Se você tiver vários consoles que compartilham um banco de dados e estão vinculado um console adicional para um banco de dados que já está atualizado, a conta de usuário você usa deve ser um membro das seguintes funções de banco de dados: db_datareader, db_datawriter, STExec e STCatalogupdate. Além disso, a conta de serviço usada para operações de segundo plano deve ser um membro da função db_owner. Se sua conta é um membro das funções de db_securityadmin e db_accessAdmin, a ferramenta de atualização do banco de dados automaticamente tentará mapear e configurar as funções necessárias para você.

PROCEDIMENTO DE ATUALIZAÇÃO

Visão geral

Esta seção descreve como atualizar do Shavlik Protect 9.0 ou do Shavlik Protect 9.1 para o Shavlik Protect 9.2. Se você está aproveitando esta oportunidade para mover o console para uma nova máquina e você deseja executar a migração usando a Ferramenta de Migração, consulte o *Guia do Usuário da Ferramenta de Migração do Shavlik Protect* antes de executar a atualização.

Antes de executar a atualização, certifique-se de ler a seção *Alterações significativas e Melhorias* na página 18 assim você está ciente de como a atualização afetará seu sistema. Você também pode querer anotar todas as suas configurações personalizadas de usuário, pois algumas não são preservadas durante a atualização (consulte a página 17).

Executando a Atualização

1. Compactar o banco de dados usado para armazenar os resultados da análise, resultados de implantação de patch e resultados de remediação de ameaça.

   Você pode fazer isso no SQL Server Management Studio clicando com o botão direito no banco de dados ShavlikScans e selecionar **Tarefas > Reduzir > Banco de dados** .
2. Criar um backup do seu banco de dados atual usando o SQL Server Management Studio.
3. Feche todos os programas em execução na máquina do console, incluindo o Shavlik Protect.
4. Faça o download do arquivo executável do Shavlik Protect 9.2 para a sua máquina de console usando o link a seguir:

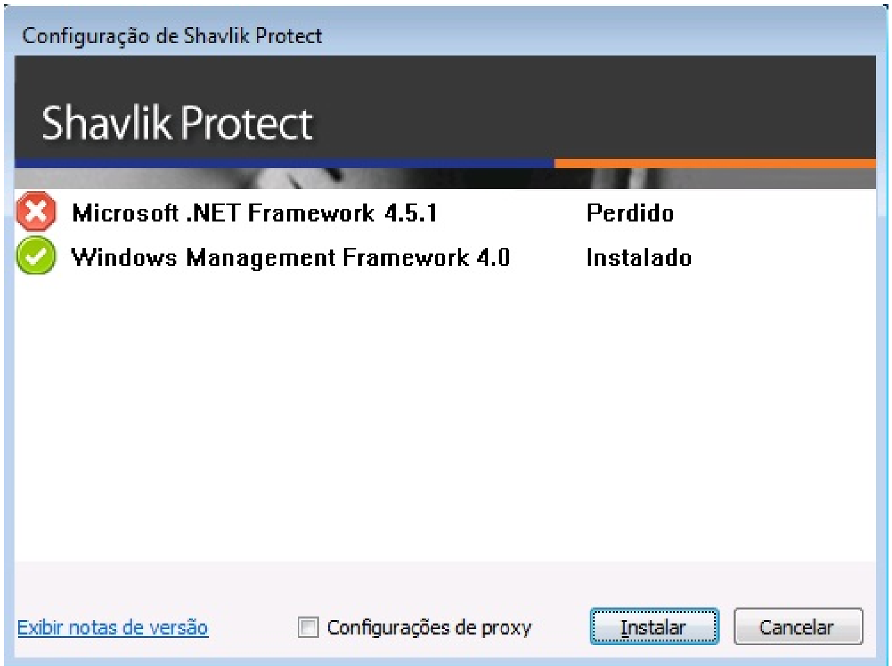
   http://www.shavlik.com/downloads/
5. Inicie o processo de instalação usando um dos seguintes métodos:
   - Clique duas vezes no arquivo chamado **ShavlikProtect.exe.**
   - Digite o nome do arquivo em um prompt de comando. Isso permite que você use uma ou mais opções de linha de comando. Você deve considerar este método se estiver atualizando um banco de dados muito grande. A opção DBCOMMANDTIMEOUT é usada para especificar o valor do tempo-limite do comando SQL durante a instalação. O valor-padrão é 15 minutos por GB. O valor mínimo de tempo-limite é o maior valor entre 15 minutos por GB ou 1800 segundos (30 minutos). Se você tiver um banco de dados de 4 GB, deverá aumentar o valor do tempo-limite para 3.600 segundos (60 minutos). Por exemplo:

     ```
     ShavlikProtect /wi:"DBCOMMANDTIMEOUT =3600"
     ```

Nota: Se receber um aviso de que é necessário reinicializar, clique em **OK**, e o processo de instalação continuará automaticamente após a reinicialização.

6. Responder para o diálogo que pergunta se você quer continuar com a atualização.

   Se você clicar em Sim e a máquina do console estiver sem um ou mais pré-requisitos, um diálogo similar ao seguinte será exibido. Se não houver pré-requisitos faltando, pule o passo a seguir e continue com o diálogo **Bem-vindo**.

7. Clique em **Instalar** para instalar quaisquer dos pré-requisitos ausentes.

   O Assistente de Configuração talvez precise executar uma reinicialização durante esta parte do processo do instalação. Se uma reinicialização é necessária, quando a máquina for reiniciada o diálogo de Configuração irá reaparecer. Basta clicar em Instalar novamente para continuar com a atualização.

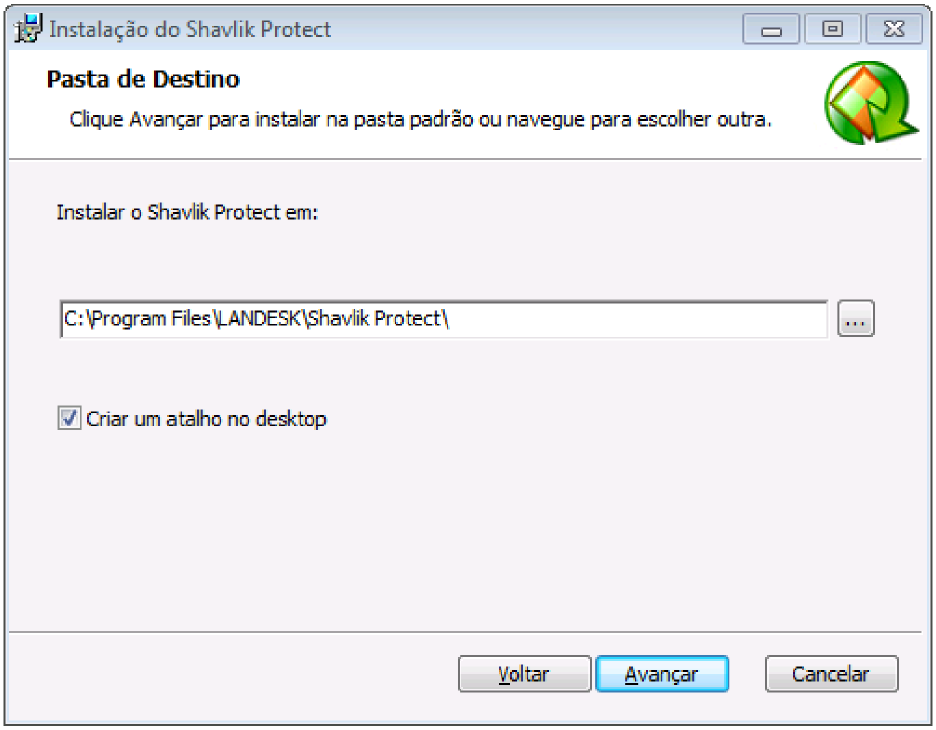
   O diálogo **Bem-vindo** é exibido.

8. Leia as informações no diálogo **Bem-vindo** e clique em **Avançar**.

   O acordo de licença é exibido. Você deve aceitar os termos do acordo da licença para instalar o programa.

9. Marque a caixa de seleção **Eu aceito os termos no Contrato de Licença** e clique em **Avançar**.

   O diálogo **Pasta de Destino** será exibido.



10. Caso deseje alterar o local-padrão do programa, clique no botão Procurar e escolha um novo local. Você também tem a opção de instalar um ícone de atalho no seu desktop. Quando tiver terminado, clique em **Avançar**.

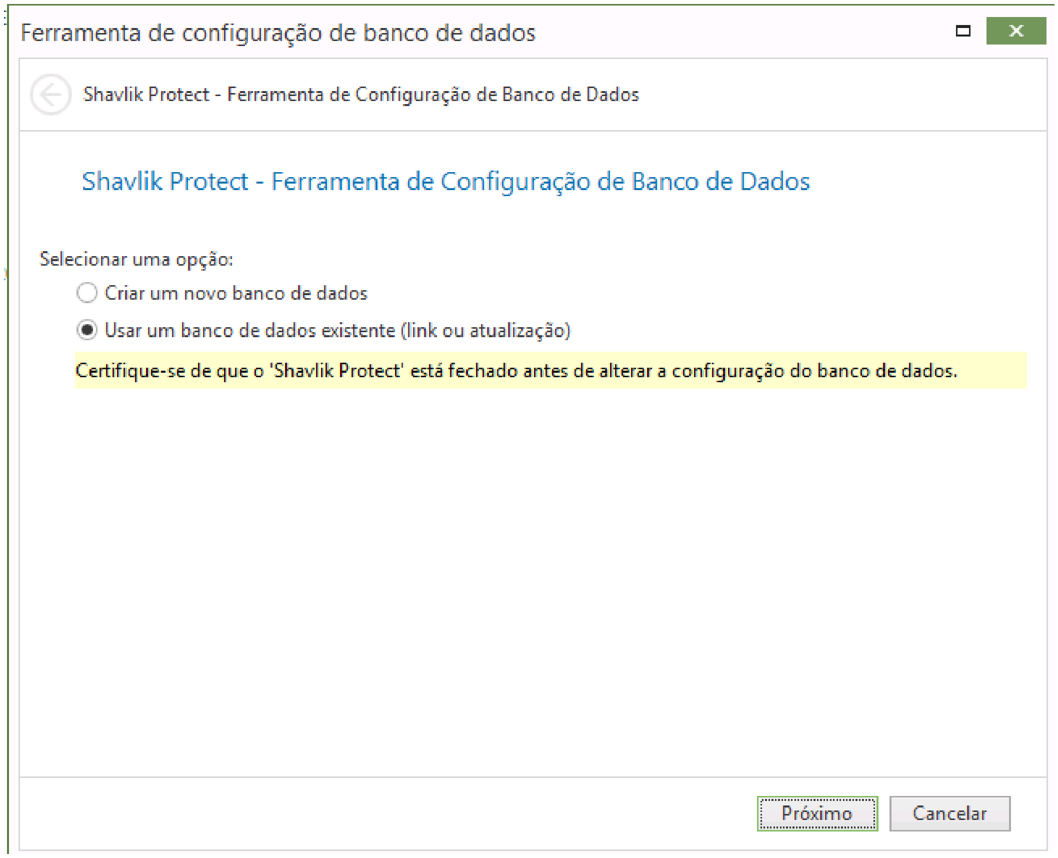
    O diálogo **Programa de Melhoria do Produto** será exibido. Leia a descrição e decida se você aceita participar do programa. O programa permite Shavlik a coletar informações de uso do produto que ajudará a melhorar as versões futuras do produto.

11. Clique em **Avançar**.

    O diálogo **Pronto para Instalar** é exibido.

12. Para iniciar a instalação, clique em **Instalar**.

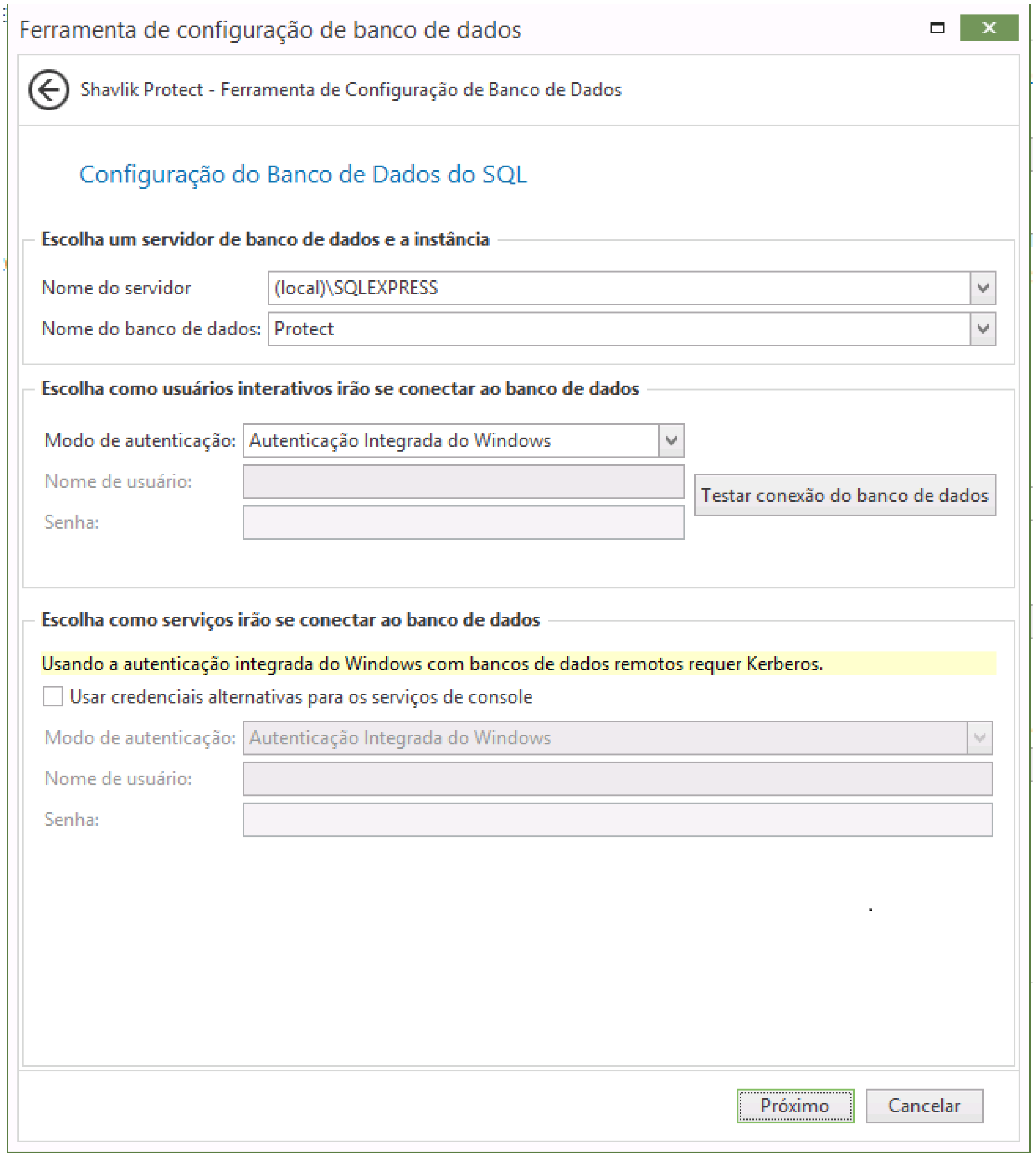
    Próximo ao fim do processo de instalação, o diálogo **Ferramenta de Configuração de Banco de Dados** será exibido.



Importante! No passo seguinte, NÃO selecione **Criar um novo banco de dados**. Se você fizer um novo banco de dados será criado e os seus dados existentes não serão usados.

13. Certifique-se que **Usar um banco de dados existente** está selecionada e, em seguida, clique em **Avançar**.

    Um diálogo semelhante ao seguinte é exibido:



14. Usar as caixas fornecidas para definir como os usuários e os serviços acessarão o banco de dados do SQL Server.

Escolha um servidor de banco de dados e a instância

- **Nome do servidor** Você pode especificar uma máquina ou você pode especificar uma máquina e a instância do SQL Server em execução nesta máquina.
- **Nome do banco de dados:** especifique o nome do banco do dados que você deseja usar. O nome do banco de dados padrão é **Protect**.

Escolha como usuários interativos irão se conectar ao banco de dados

Especifique as credenciais a serem usadas pelo programa quando o usuário executar uma ação que exija acesso ao banco de dados.

- **Autenticação Integrada do Windows:** Esta é a opção recomendada e padrão. Shavlik Protect usará as credenciais do usuário conectado no momento para se conectar ao banco de dados do SQL Server. As caixas de **Nome de Usuário** e **Senha** estarão indisponíveis.
- **Usuário do Windows Específico:** Selecione esta opção apenas se o banco de dados do SQL Server está em uma máquina remota. Esta opção não terá efeito se o banco de dados está na máquina local (console). (Consulte *Fornecimento de credenciais* na **Guia de administração do Shavlik Protect** para obter mais informações sobre as credenciais da máquina local.) Todos os usuários do Shavlik Protect usará as credenciais fornecidas ao executar as ações que necessitam de interação com banco de dados do SQL Server remoto.
- **Autenticação do SQL:** Selecione esta opção para inserir uma combinação específica do nome de usuário e senha ao fazer logon no servidor SQL especificado.

  Cuidado! Se você fornecer credenciais de autenticação do SQL e não implementou a criptografia SSL para conexões do SQL, as credenciais serão passadas pela rede em texto não criptografado.
- **Testar conexão do banco de dados:** Para verificar que o programa pode usar as credenciais de usuário interativo fornecido para conectar ao banco de dados, clique neste botão.

Escolha como serviços irão se conectar ao banco de dados

Especifique as credenciais que você deseja que os serviços de segundo plano usem ao fazer a conexão com o banco de dados. Estas são as credenciais que o importador de resultados, várias operações de agente e outros serviços irão usar para fazer logon no SQL Server e fornecer os status.

- **Usar credenciais alternativas para os serviços de console:**
  - Se o banco de dados do SQL Server estiver instalado na máquina local, você normalmente ignorará esta opção não habilitando esta caixa de seleção. Neste caso as mesmas credenciais e o modo de autenticação que você especificou acima para os usuários interativos serão usados.
  - Você normalmente irá apenas habilitar esta caixa de seleção se o banco de dados do SQL Server está em uma máquina remota. Quando o banco de dados está em uma máquina remota, você precisa de uma conta que possa ser autenticada no banco de dados do servidor remoto.
- **Método de autenticação:** Disponível somente se **Usar credenciais alternativas para os serviços de console** está habilitada.
  - **Autenticação Integrada do Windows:** Selecionar esta opção significa que a conta de máquina será usada para conectar ao SQL Server remoto. O protocolo de autenticação de rede Kerberos deve estar disponível para transmitir com segurança as credenciais. As caixas de Nome de Usuário e Senha estarão indisponíveis.

Nota: se você escolher **Autenticação Integrada do Windows,** o programa de instalação tentará criar um logon do SQL Server para a conta da máquina. Se o processo de criação da conta falhar, consulte *Notas de Pós-Instalação do SQL Server* no *Guia de Instalação do*

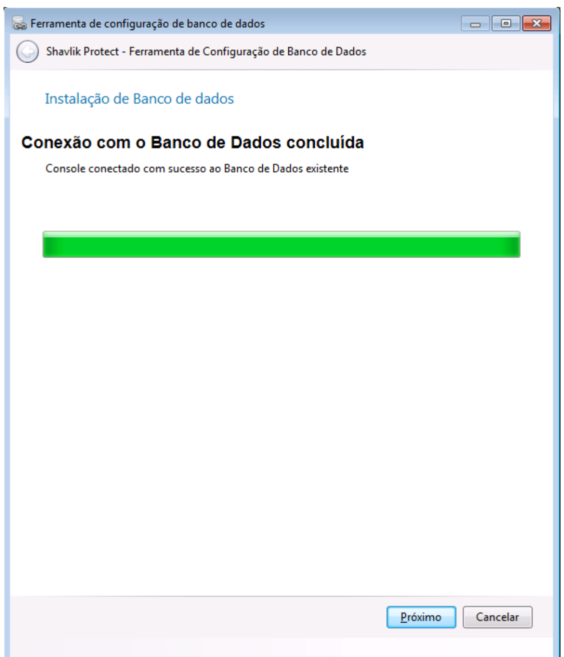
Shavlik Protect 9.2 para obter instruções sobre como configurar manualmente um servidor SQL remoto para aceitar credenciais de conta de máquina. Fazer isso depois de concluir o processo de atualização do Shavlik Protect porém antes de você iniciar o programa.

- **Usuário do Windows Específico:** Selecione esta opção para inserir uma combinação específica do nome de usuário e senha. Serviços de segundo plano do Shavlik Protect usará essas credenciais para se conectar ao banco de dados do SQL Server. Esta é uma boa opção de fallback se por algum motivo você tem dificuldades na implementação de autenticação integrada do Windows.
- **Autenticação do SQL:** Selecione esta opção para fornecer uma combinação específica do nome de usuário e senha para os serviços usarem quando fazer logon no servidor SQL.

15. Depois de fornecer todas as informações necessárias, clique em **Avançar**.

Nota: Se o programa de instalação detectar um problema com qualquer uma das credenciais especificadas, uma mensagem de erro será exibida. Isso geralmente indica que a conta de usuário que você especificou não existe. Faça a correção e tente novamente.

O console está conectado ao seu banco de dados existente. Quando o processo de link é concluído o seguinte diálogo é exibido.



16. Clique em **Avançar**.
17. No diálogo **Instalação Completa** clique em **Concluir**.
18. No diálogo **Concluiu o Assistente de Configuração do Shavlik Protect**, habilitar a caixa de seleção **Iniciar Shavlik Protect** e, em seguida, clique em **Concluir**.

ATUALIZAR AS TAREFAS EXECUTADAS NO CONSOLE

Para concluir a atualização, as tarefas seguintes devem ser executadas no console do Shavlik Protect.

Atribuir Credenciais do Agendador

Agora é necessária uma credencial de agendador que corresponda à sua conta de usuário atual para executar tarefas de console agendadas. Se houver tarefas agendadas no console e a credencial do agendador não tiver sido definida, você receberá um aviso no momento da inicialização para definir a credencial. Essa verificação ocorre toda vez que o Shavlik Protect é iniciado, a fim de assegurar que as tarefas agendadas continuem sendo executadas.

Examine suas Tarefas Agendadas

As tarefas agendadas agora são monitoradas e gerenciadas a partir de duas áreas separadas. Você deve analisar ambos os gerenciadores de tarefas agendadas para verificar se suas tarefas existentes foram adequadamente transportadas.

- O **Gerenciador de Tarefas de Console Agendadas** fornece um local para a exibição das tarefas atualmente agendadas no console, como análises de patches, análises de ativos, implementação de patches na máquina do console, execução de scripts e relatórios agendados.
- O **Gerenciador de Tarefas Remotas Agendadas** fornece um local para a exibição de tarefas de energia e de implementação de patches atualmente agendadas em máquinas-alvo remotas.

Atualizar Sua Licença (Apenas Consoles Offline)

Se o seu console está offline (sem conexão com a Internet), você precisa atualizar manualmente sua licença para exibir e usar os novos recursos no Shavlik Protect 9.2. Para obter mais informações sobre como ativar um console desconectado, no sistema de Ajuda consulte **Instalação e Configuração > Introdução > Ativando o Programa**.

Se o console está online a licença será atualizado automaticamente durante o processo de atualização.

Revise os modelos de análise de patch existentes e os grupos de patches

Há três problemas a serem considerados nessas áreas.

- **Modelos de Análise de Patches:** A guia **Filtragem**, no diálogo **Modelo de Análise de Patches**, foi atualizada para permitir maior precisão durante a análise. Embora o processo de atualização converta automaticamente os modelos de análise existentes para o novo estilo, você deve conferir seus modelos para verificar se há alterações.
- **Grupos de Patches:** Os grupos de patches não são mais definidos por meio de um diálogo separado; agora eles são criados e gerenciados de dentro da Exibição de Patches. Embora o processo de atualização converta automaticamente os grupos de patches existentes para a nova convenção, você deve conferir os grupos para verificar se há alterações. Seus grupos de patches podem estar menores após a atualização, pois o Shavlik descontinuou o suporte para muitos patches antigos.

- **Grupos de Patches gerados automaticamente e modificados:** Para preservar o comportamento dos modelos de análise de patches, um ou mais dos grupos de patches existentes podem ser modificados durante o processo de atualização e um ou mais novos grupos de patches podem ser gerados automaticamente.
    - **Criando Grupos de Patches:** Se você faz referência a um grupo de patches dentro da seção **Configurações do filtro de patch** do modelo de análise de patch 9.0 ou 9.1 e **Análise selecionada** estiver desabilitada, qualquer patch que não atender ao critério definido pelos filtros do modelo de análise serão removidos do grupo. Eis o porquê: No Protect 9.0 ou 9.1, os filtros de modelos de análise podem mascarar o fato de que o grupo de patches possa conter tipos de patch que você nunca teve a intenção de analisar ou implantar. No Protect 9.2, quando o grupo de patches é usado como uma linha de base, os filtros do modelo de análise não serão aplicados e as imprecisões nos grupos de patches podem ser reveladas. Se o processo de atualização detectar esta situação, ele será automaticamente modificado para preservar a interação pretendida entre o modelo de análise e o grupo de patches.

      Exemplo:

      Suponha que o grupo de patches 9.1 contenha uma mistura de patches de Segurança, Não segurança e Distribuição de software. No modelo de análise que é referência para este grupo de patches, a seção **Configurações do filtro de patch** é definida como **Análise selecionada** e a seção **Propriedade de patches** é definida para detectar apenas patches de Segurança. Nesta configuração, o filtro **Propriedades de patch** será respeitado e apenas patches de segurança serão detectados (apesar de o grupo de patches conter patches de Não segurança e Distribuição de software).

      Após ser atualizado para o 9.2, o modelo de análise definirá o grupo de patch como uma linha de base e todos os filtros do modelo de análise serão ignorados. Se o grupo de patches não for modificado, os patches de Não Segurança e Distribuição de software agora serão detectados (e habilitados se você selecionar a caixa de verificação **Auto-implantar patches após análise** quando realizar a análise). O processo de atualização reconhecerá esta discrepância e removerá os patches de Não segurança e Distribuição de software do grupo de patches.

      Nota: Continuando, tenha cuidado para gerenciar adequadamente seus grupos de patches ao não adicionar patches ou tipos de patches desnecessários ou indesejados.

- **Grupos de Patches gerados automaticamente:** Uma cópia de um grupo de patches existente será automaticamente gerada pelo processo de atualização se todas as condições forem atendidas:
  - Se o grupo de patches for tido como referência dentro da seção **Configurações do filtro de patch** de um modelo de análise de patch e **Análise selecionada** estiver habilitada, e
  - Se o grupo de patches for tido como referência por uma política de agente ou por um segundo modelo de análise que contém diferentes definições de filtro, e
  - Se o grupo de patches tiver que ser modificado pelo processo de atualização para manter a compatibilidade (veja acima)

  Nesta situação, uma cópia do grupo de patches será gerada e modificada como descrito acima. O nome do novo grupo de patches será ***<nome do grupo de patches> -gerado para <nome do modelo de análise>**. O(s) modelo(s) que servem como referência para o grupo de patches será atualizado para usar o novo grupo de patch. O grupo de patches original é preservado para que as referências a ele oriundas das políticas de agente ou outros modelos de análise sejam mantidas.

  Você deve revisar as modificações e, se desejado, renomear o grupo de patches gerado automaticamente para um nome mais amigável ou mais significativo.

Atribuir Alias ao Console

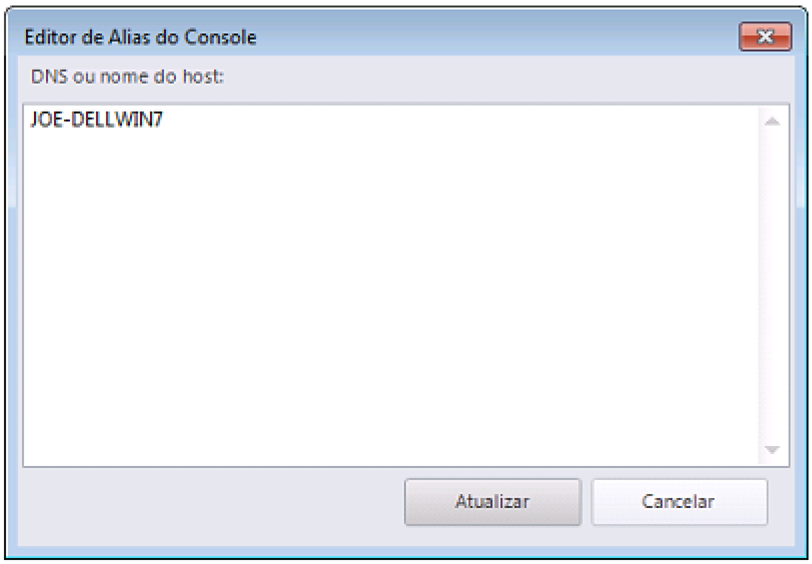
Esta tarefa é necessária se uma ou mais das condições a seguir forem aplicáveis:

- Você atribuiu a máquina de console para um novo domínio
- Você deu ao console um novo nome comum ou endereço IP
- Você instalou agentes manualmente, e eles usam um endereço IP para se comunicar com o console

Sob estas condições você deve usar a ferramenta **Editor de Alias do Console** para identificar os nomes ou endereços antigos do console como alias de confiança. Caso contrário, quando um agente fizer check-in no console do Shavlik Protect ou quando uma máquina sem agente tentar enviar mensagens de status da implementação de patches ao console, eles não conseguirão verificar se a máquina contatada é confiável.

1. Selecione **Ferramentas > Editor de alias do console**.

   O diálogo **Editor de Alias do Console** é exibido. Ele irá conter os nomes e os endereços IP usados atualmente para identificar a máquina de console. Por exemplo:

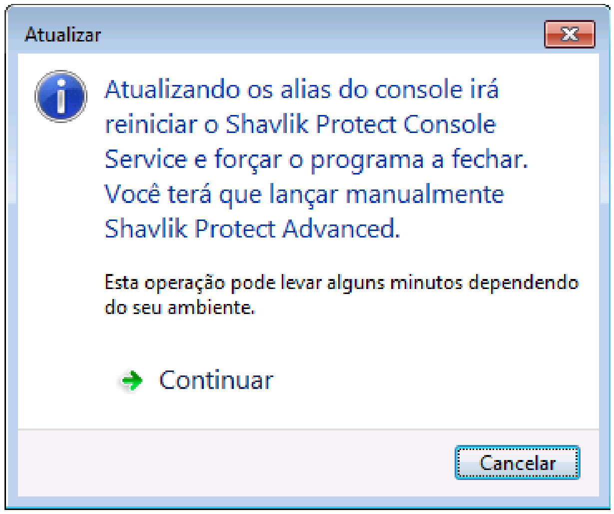
   

2. Digite os nomes e/ou os endereços IP que você deseja usar como um alias para a máquina de console.

   Você pode especificar endereços IP usando o formato de um IPv4 ou IPv6.

3. Clique em **Atualizar**.

   O seguinte diálogo é exibido:



Para atualizar os alias do console o serviço de console deve ser reiniciado e Shavlik Protect deve ser fechado e reiniciado manualmente.

IMPORTANTE! Os agentes não reconhecerão um novo alias até depois de fazer o check-in com o console reiniciado. O check-in deve ser iniciado por um agente seja manualmente usando o programa de cliente de agente ou através de um check-in agendado; um comando de check-in emitido pelo console para um agente não irá atualizar o certificado do console.

Sincronizar seus Servidores de Distribuição

Você deve atualizar o seu servidor de distribuição com os patches mais recentes e/ou mecanismos de análise e arquivos de definição XML contidos no console. Isto é particularmente importante se seus agentes usam servidores de distribuição para download esses arquivos. Os servidores de distribuição devem ser sincronizados com os arquivos de console atualizado **antes** dos agentes executarem seu check-in.

Para sincronizar seus servidores de distribuição:

1. Selecione **Ajuda > Atualizar os arquivos** para certificar-se que o console contém todos os arquivos mais recentes.
2. Selecione **Ferramentas > Operações > Servidores de Distribuição**.
3. Na caixa **Adicionar sincronização agendada** no painel superior, selecione o componente que você deseja sincronizar.
4. No painel superior, selecione qual o servidor de distribuição que deseja sincronizar com o console.
5. Clique em **Adicionar sincronização agendada**:
6. Especificar quando você deseja que a sincronização ocorra e clique em **Salvar**.
7. No painel **Agendar sincronização automática**, selecione a entrada de sincronização agendada.
8. Clique em **Executar agora**.

Não se preocupe se os agentes fizerem check-in antes de você ter concluído a sincronização dos servidores de distribuição. Os agentes serão atualizados na próxima vez que uma tarefa agendada é executada ou o agente atualiza seus binários.

Considere Habilitar o Recurso Patch Preditivo

Este novo recurso permite ao Shavlik Protect baixar automaticamente os patches que provavelmente serão implementados em um futuro próximo. Caso você use servidores de distribuição, pode sincronizar o Patch Preditivo com seus servidores de distribuição para que eles recebam cópias dos patches baixados. A opção Patch Preditivo é habilitada em **Ferramentas > Operações > guia Downloads** e é sincronizada com seus servidores de distribuição por meio da opção **Sincronizar com Patch Preditivo**, no diálogo **Servidor de Distribuição**. Consulte o sistema de Ajuda para obter detalhes completos.

Restabelecer a Segurança Entre os Seus Consoles de Rollup de Dados

Se você usa vários consoles e tem uma configuração de rollup de dados no lugar, você deve restabelecer a associação de segurança entre o console central e cada console remoto.

IMPORTANTE! Uma vez iniciado o processo de atualização, nenhuma atividade de rollup de dados ocorrerá até que o console central e o console remoto sejam atualizados e a associação de segurança entre os dois consoles seja restabelecida. Por esta razão é altamente recomendável que você atualize seus consoles em tandem e num momento em que se espera muito pouca atividade de rollup de dados.

No Console Central

1. Atualize o console central.
2. Selecione **Ferramentas > Operações > Rollup de Dados** e verifique se a caixa de seleção **Aceitar e importar resultados de um remetente de rollup** está habilitada.

Em Cada Console Remoto

1. Atualize cada console remoto.
2. Selecione **Ferramentas > Operações > Rollup de Dados**.
3. Verifique o endereço IP/nome de host e os valores de porta do console de rollup.
4. Clique em **Registrar**.

Para obter mais informações sobre o rollup de dados, no sistema de Ajuda, consulte **Gerenciando Múltiplos Consoles > Configuração de Rollup de Dados.**

Analise suas Máquinas Virtuais

Se você tiver máquinas virtuais definidas em um grupo de máquinas, seja na guia **Máquinas Virtuais Hospedadas** ou na guia **Máquinas Virtuais da Estação de Trabalho**, você deve, após realizar a atualização, iniciar uma análise dessas máquinas a partir da página inicial ou de dentro do grupo de máquinas. Você precisa fazer isso para restabelecer as identidades das máquinas com o Protect. Se você não executar a análise, os campos **Servidor Virtual** e **Caminho** podem não ser exibidos na Exibição de Máquinas, e as implementações nessas máquinas vão falhar.

Verifique suas Configurações Personalizadas de Usuário

As configurações personalizadas de usuário a seguir não são preservadas durante a atualização.

- Ferramentas > Opções > guia Exibir:
  - Item recente (dias)
  - Itens de arquivo
  - Mostrar apenas os itens criados por mim
  - Mostrar newsfeed principal
  - Mostrar itens informativos nos resultados da Análise de patch
  - Mostrar service packs em Exibir > Patches
- Ferramentas > Opções > guia Notificações e Avisos:
  - Avisar antes de agendar implementações
  - Fechar Arquivos de Atualização quando terminar
  - Avisar se sincronização de Protect Cloud não está habilitado para este console
  - Avisar antes de abrir 7 ou mais boletins
- Ferramentas > Opções > guia Log:
  - Diagnóstico de análise de patches
- Rastreador de Implementação:
  - Atualizar velocidade
  - Dias para mostrar
  - Mostrar falhas
  - Mostrar em andamento
  - Mostrar concluído com êxito
- Diálogo Relatórios
  - Ordenar por ID de IAVA
- Guia Boletins do Hipervisor ESXi:
  - Apenas mostrar o mais recente
- Histórico de Eventos
  - Limitar resultados para anteriores (dias)
- Exibição de Resultados de ITScripts
  - Resultados desde

Saiba que o Protect 9.2 Usa um Certificado Raiz SHA-2

O Shavlik está introduzindo o uso de certificados SHA-2 de raiz e console no Protect 9.2. Há duas razões principais para isso: os certificados SHA-2 de 2048 bits são mais seguros que os antigos SHA-1 de 1024 bits, e os certificados raiz SHA-1 estão sendo descontinuados e não serão mais aceitos pelo Windows a partir de 1º de janeiro de 2017.

Depois que você concluir o processo de atualização, o Shavlik Protect 9.2 começará seu próprio processo nos bastidores para emitir novos certificados SHA-2 de raiz e console. Se você não estiver usando agentes, esse processo será invisível para você e poderá ser ignorado. Se estiver usando agentes, parte do processo envolve aguardar que seus agentes façam check-in para receber o novo certificado raiz. Esse processo pode levar alguns dias ou semanas, dependendo de vários fatores, mas tudo se desenrolará em segundo plano. Seu único envolvimento pode ser monitorar o log do Histórico de Eventos para ver se ocorreu algum problema que exija sua atenção.

ALTERAÇÕES E MELHORIAS SIGNIFICATIVAS NO SHAVLIK PROTECT 9.2

Os detalhes completos sobre cada um dos tópicos a seguir podem ser encontrados no sistema de Ajuda:

http://help.shavlik.com/Protect/onlinehelp/92/ENU/PRT.htm

Implantações de Patch

O mecanismo de embalagem e de implementação de patches nas máquinas foi completamente reescrito. O desempenho e a confiabilidade foram melhorados.

Conteúdo do Patch

Os dados de implementação e avaliação de patches que o Shavlik Protect consome foram reembalados e aprimorados de várias maneiras.

Filtragem de Modelos de Análise de Patches

Mais metadados foram adicionados ao conteúdo do patch. Além disso, a guia **Filtragem**, no diálogo **Modelo de Análise de Patches**, foi atualizado para permitir mais precisão durante a análise.

Exibição de Patches/Grupo de Patches

A Exibição de Patches foi completamente redesenhada e atualizada. Ela tira proveito do novo formato de conteúdo, permitindo a você exibir as informações dos patches de uma forma mais concisa. Além disso, os grupos de patches agora são criados e gerenciados dentro da Exibição de Patches. Isso permite a você pesquisar patches e criar grupos de patches de maneira mais unificada.

Tarefas Agendadas

As tarefas agendadas no console agora usam o Agendador de Tarefas da Microsoft. Um novo diálogo, disponível no menu **Gerenciar > Tarefas de Console Agendadas**, permite a você exibir e gerenciar essas tarefas.

Relatórios

Um novo relatório **Fim de Vida por Produto** está disponível. Além disso, um novo diálogo **Agendar Relatório**, disponível no menu **Ferramentas > Agendar Relatório**, permite a você gerar automaticamente um relatório em algum momento no futuro. O relatório pode ser automaticamente gerado uma única vez ou de forma recorrente.

Patch Preditivo

Esta nova opção permite ao Shavlik Protect baixar automaticamente patches que provavelmente serão implementados em um futuro próximo. Baixar os patches antes da implantação ajudará a agilizar o processo de implantação.

Patch Tuesday + Adiamento de X (dias)

Ao agendar análises de console, você agora pode adiar uma análise recorrente por um certo número de dias para coincidir com um evento regular. Por exemplo, você pode agendar uma análise mensal de patches para ocorrer no dia seguinte à Patch Tuesday utilizando a nova opção **Postergar (dias)**.

Notificação do Fim de Vida

De agora em diante, se a versão do Shavlik Protect que você está usando se aproximar de sua data de fim de vida (EOL), uma notificação será exibida quando o Shavlik Protect for iniciado.

Integração com o Protect Cloud

Os resultados de análise e implementação de patches podem ser enviados periodicamente ao Protect Cloud. Se você for usuário do Shavlik Empower, os dados de patch serão recuperados periodicamente do Protect Cloud pelo Empower e poderão ser exibidos por meio de uma interface de usuário do Shavlik Empower no navegador.

Alterações na interface de usuário

Os seguintes itens da interface de usuário foram alterados:

- A Exibição de Patches foi completamente redesenhada.
- Grupos de patches agora são criados e gerenciados dentro da Exibição de Patches.
- Na Exibição de Máquinas:
    - O painel superior agora contém três novas colunas: Servidor Virtual, Nome da VM e Caminho
    - A guia **Ativos Virtuais** foi removida do painel intermediário
    - No painel inferior, as guias **Máquinas Ausentes** e **Máquinas Instaladas** foram combinadas em uma nova guia, chamada **Máquinas Afetadas**.
- No modelo de implementação de patches:
    - O suporte a Mídia Original e a Pontos de Instalação do Office foi removido.
    - As opções **Fazer backup de arquivos para desinstalação** e **Modo Silencioso** foram removidas; agora elas estão sempre habilitadas
    - A guia **Servidores de Distribuição** foi redesenhada para ajudar a identificar a ordem na qual as fontes de download serão usadas
- No modelo de análise de patches:
    - A guia Filtragem foi completamente redesenhada
    - A criticidade de usuário foi removida
    - A guia Distribuição de Software mostra apenas produtos que não foram substituídos
- Em uma política de agente, todas as tarefas agora podem ser criadas sem um agendamento recorrente. Isso permite a você definir tarefas que serão executadas apenas via interface de usuário do agente ou por iniciação remota de tarefas a partir do console.
- Em um grupo de máquinas, as opções **Testar Existência** e **Testar Credenciais** foram combinadas e são implementadas pela execução de uma análise de status de energia.
- Resumos de ativos virtuais não estão mais disponíveis dentro da Exibição de Máquinas. Todas as informações de ativos virtuais agora estão disponíveis por meio do recurso Inventário Virtual.

- Removidos os relatórios Detalhe de Hardware das Máquinas Virtuais, Uso de Memória das Máquinas Virtuais e Uso de Disco das Máquinas Virtuais.
- Na Exibição de Análises, o subpainel Resumo de Análise não é mais recolhível
- As tarefas agendadas agora estão separadas em dois diálogos: **Gerenciar > Tarefas Remotas Agendadas** e **Gerenciar > Tarefas de Console Agendadas**
- Em **Ferramentas > Opções**:
  - **Exibir:** contém uma nova caixa de seleção chamada **Mostrar service packs em Exibir > Patches**
  - **Notificações e Avisos:** contém uma nova caixa de seleção chamada **Avisar antes de abrir 7 ou mais boletins**; removida a caixa de seleção **Avisar antes de agendar operações quando as Credenciais-Padrão não corresponderem ao usuário atual**
  - **Idiomas do Patch:** esta guia foi removida. O programa agora detecta automaticamente os idiomas usados pelo sistema operacional em suas máquinas gerenciadas e faz o download do arquivo de patch apenas nas versões de idioma necessárias.
  - **Análises:** contém uma nova caixa de seleção chamada **Sempre aplicar exclusões a grupos de máquinas**
  - **Implementação:** a opção **Endereço do Rastreador de Implementação** foi removida. O endereço agora é definido usando-se o **Editor de Alias do Console**.
  - **Log:** contém uma nova caixa de seleção chamada **Análise diagnóstica de patches**